UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,560	11/14/2003	Richard Bussiere	ENI-037	8242

35557 7590 01/09/2008

CHRIS A. CASEIRO
VERRILL DANA, LLP
ONE PORTLAND SQUARE
PORTLAND, ME 04112-0586

EXAMINER	
BROWN, CHRISTOPHER J	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
01/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

AK

Office Action Summary	Application No.	Applicant(s)	
	10/713,560	BUSSIERE ET AL.	
	Examiner	Art Unit	
	Christopher J. Brown	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/29/07*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,8-15,28-30 and 32-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,8-15,28-30 and 32-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

The affidavits filed on 10/29/2007 under 37 CFR 1.131 has been considered but is ineffective to overcome the Sung US 2004/0215972 reference.

An effective 1.131 must clearly identify the elements of the claims with proper dated evidence including the claimed elements. The current evidence does not identify what portions relate to which claims in the invention.

Applicants arguments regarding USC 112 rejections are persuasive.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5, 8-15, and 28-30, 32-41 are rejected as best understood under 35 U.S.C. 103(a) as being unpatentable over Huff et al International Publication No. WO 99/57625 (hereinafter "Huff") and Sung et al United States Patent Application Publication No. 2004/0215972 A1 (hereinafter "Sung").

Huff teaches a distributed intrusion detection method and manner of responding to such but fails to explicitly teach excluding intrusion detection functions from at least one or more interconnection devices.

However, in related art, Sung teaches a system for distributed intrusion detection using intelligent agents wherein the agents are selectively distributed. (Sung paragraphs 83, 85, 95, 101)

Sung teaches that is a desirable feature to be able to dynamically distribute agents to selected locations (Sung paragraph 101).

The combination of these two systems clearly represents the teachings of Huff wherein agents are dynamically distributed to nodes and not distributed to every node in order to provide for a more efficient system as outlined by Sung.

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Sung with Huff in order to provide for a more scalable efficient implementation based upon network size, traffic conditions, and computational load.

Regarding Claim 1: A method of responding to the detection of an intrusion on a network system that provides network services, the network system including one or more attached functions and a plurality of interconnection devices, the method comprising the steps of: a. establishing signal transfer policies for each of the plurality of interconnection devices; (Huff Fig 3-4, pg 4 line 11 – pg 7 line 11, pg 13 lines 10-12, pg 14 lines 6-12, pg 15 lines 3-11, pg 17 lines 14-25, pg 18 lines 1- pg 19 line 25)

monitoring the network system for intrusions (Huff Abstract, Fig 1, 3, pg 5 lines 2-5)

excluding from at least one of the plurality of interconnection devices a policy enforcement modual for effecting signal transfer policy changes; (Sung paragraphs 83, 85, 95, 101)

upon detection of one or more intrusions of the network, selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions (Huff pg 5 lines 6-9, 12-16, pg 12 line 29 – pg 13 line 3, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13)

Identifying the source of the intrusion occurs two fold within the system of Huff by not only detecting the device on the local network where the issue arises but by tracing the remote location as well.

Regarding Claim 2: The method as claimed in Claim 1 wherein the step of identifying one or more sources of the intrusions, including the step of identifying a physical address or a logical address of each of the one or more identified sources (Huff pg 8 lines 24-30, pg 11 lines 5-23, pg 12 line 30 – pg 13 line 2, 23-27, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13)

Regarding Claim 3: The method as claimed in Claim 2 wherein the physical address information is a MAC address or the logical address information is an IP address (Huff pg 8 lines 24-30, pg 11 lines 5-23, pg 12 line 30 – pg 13 line 2, 23-27, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13) As provided by Huff the use of Ethernet type networks dictates that for address resolution purposes, which is an inherent functionality of such a network, addresses are stripped from packets which contain both MAC and IP type addresses. Furthermore, as stated since all devices are addressable on the network and the implementation of any such protocol as TCP/IP dictates resolution of such devices occurs via a MAC address associated to an IP address.

Regarding Claim 4: Including in at least one of the plurality of interconnection devices the capability for such interconnection devices to change directly their own signal transfer policies (Huff pg 4 lines 8- pg 5 line 10)

Regarding Claim 5: Employing an intrusion detection device of the network system to perform the function of detecting the one or more intrusions, wherein the intrusion detection device is either a centralized network infrastructure device or a plurality of distributed network system devices (Huff Fig 3, pg 4 line 11 – pg 7 line 11, pg 11 lines 25-30; Sung paragraph 28) the intrusion detection function is centralized by the security server that controls actions taken by the distributed agents in effect being both centralized and distributed.

Regarding Claims 8, 28, 29: The method as claimed in Claim 2 the step of identifying one or more of the plurality of interconnection devices associated with the one or more identified sources of intrusions, including the step of determining the physical address, logical address, or both for each of the identified one or more interconnection devices (Huff pg 8 lines 10-30, pg 11 lines 5-23, pg 12 line 30 – pg 13 line 2, 23-27, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13) Resolution of addresses in order to send messages and communicate actions must take place via such a path.

Verifying the Identity of the identified one or more sources (Huff pg 5 lines 1-10; Sung paragraphs 109-133) as taught by both Huff and Sung there are measures for tracking the source of the intrusion.

Regarding Claim 9: The method as claimed in Claim 2 further comprising the step of verifying the identification of the identified one or more sources (Huff pg 5 lines 6-9, 12-16, pg 12 line 29

– pg 13 line 3, pg 18 line 27 – pg 19 line 13, pg 20 lines 3-5, pg 21 lines 10-13) Huff states that agents serve to verify the identity of the source through the steps of tracing.

Regarding Claim 10: The method as claimed in Claim 1 wherein the step of selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions includes the step of configuring the one or more interconnection devices to perform one or more functions selected from the group consisting of: blocking complete access to the network services by the identified one or more sources of a detected intrusion, blocking access by identified logical addresses only, blocking access by an identified access protocol only, limiting bandwidth, limiting exchanges to or from the identified one or more interconnection devices, to or from one or more other devices of the network system, or to or from any of the attached functions not identified as an intrusion source (Huff pg 4 line 11 – pg 7 line 11, pg 18 line 1 –pg 19 line 25, pg 22 lines 3-20; Sung paragraphs 19-21, 79, 108) The intruder is either disabled through policy changes or is misdirected toward information that cannot be harmed in order to collect further information about the intruder. and directing all signals exchanged by the identified one or more sources to a honey-pot, an intrusion detection device, a monitoring device, or a simulation device (Huff pg 18 line 1 –pg 19 line 25, pg 20 lines 2-8, pg 20 lines 27- pg 21 line 1, pg 21 lines 10-30, pg 22 lines 3-20) The intrusion system directs all information back to the central server which stores information within a database, and also as outlined provides for misdirecting the intruder in order to collect further information.

Regarding Claim 11: The method as claimed in Claim 1 wherein the step of selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in

response to the one or more detected intrusions includes the step of configuring the identified one or more interconnection devices to permit connectivity of the identified sources of a detected intrusion while dampening the level of activity associated with the identified one or more sources to minimize network harm while permitting analysis and auditing of the identified one or more sources and the gathering of forensic evidence (Huff pg 17 line 18 – pg 19 line 14, pg 21 line 6 – pg 22 line 19; Sung paragraph 108) as recited the intruder is misdirected toward data to decrease any possible harm to the network in order to collect data about the attacker.

Regarding Claim 12: The method as claimed in Claim 1 wherein the step of selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions includes the steps of first configuring a first set of the one or more interconnection devices with a first set of one or more policy changes, monitoring the network system for intrusions and, upon detection of one or more intrusions related to the intrusions causing the first one or more policy changes, configuring a second set of the one or more interconnection devices with a second set of one or more policy changes (Huff pg 17 line 18 – pg 19 line 14, pg 21 line 6 – pg 22 line 19; Sung paragraph 108) Audit levels may be changed as well as having the attacker misdirected for further examination. Upon detection of further activity from the increase in auditing further actions can be taken by the system to have the attacker disabled or misdirected through policy changes on the specific devices.

Regarding Claim 13: The method as claimed in Claim 12 wherein one or more of the one or more interconnection devices of the second set are interconnection devices of the first set (Huff fig 3, pg 15 lines 3-11, pg 17 lines 8-22, pg 18 lines 1-12, pg 19 lines 1-14) The system has

agents on nodes that monitor for intrusions, when an intrusion or suspicious activity is detected the audit level can be increased and upon further inspection if such activity is determined to be inappropriate further action can be taken by the agent.

Regarding Claim 14: The method as claimed in Claim 1 wherein the one or more interconnection devices are network entry devices (Huff Fig 1, page 8 lines 10-14, 20-30, pg 9 lines 12-15, pg 13 lines 24-26) Such devices as servers, hosts, and any other well-known network addressable nodes are anticipated by Huff as containing the agents, such devices as firewalls, VPNs and switches/routers are embodied as network computing devices and thus are anticipated by the present invention.

Regarding Claim 15: The method as claimed in Claim 1 wherein the one or more policy changes are configured on one or more ports of one or more of the identified one or more signal transferring devices (Huff pg 14 lines 26—pg 15 line 2) Huff provides for configuring agents through associated ports.

Regarding Claim 33: a directory service function for receiving address information for attached functions and interconnection devices; (Huff Fig 4, pg 18 lines 15-26) Huff provides a directory of all monitored devices and there associated enforcement mechanisms.

Regarding Claim 34: a policy manager function for configuring interconnection devices of the network infrastructure with policies (Huff Fig 4, pg 18 lines 15-26) There are means associated with the directory for changing policies and also within the automatic response for implementing and changing policies.

Regarding Claim 35: Policy decision function configured: a. to receive detected intrusion information from the intrusion detection functions;

To receive information from the directory service functions;

To evaluate whether a policy change or changes is or are required on one or more of the interconnection devices in response to the detected intrusion information; and to direct the policy manager functions to configure one or more of the plurality of interconnection devices with determined policy changes upon deciding to do so based upon the evaluation. (Huff figure 3, page 5 lines 10-16; Sung paragraph 108) Clearly the centralized server of Huff performs the correlate between agents and response when an automatic response present and further Sung anticipates such changes as detailed by the dynamic distribution of agents and the learning response of the system.

Regarding Claim 36: The policy manager function and the policy decision function are part of a centralized server. (Huff figure 3) Huff provides for both the distributed and centralized policy decisions.

Regarding Claim 37: The directory service function is part of the central server (Huff Figure 3)

Regarding Claim 38: The intrusion detection function is a centralized intrusion detection function or a distributed intrusion detection function (Huff Figure 3)

Regarding Claim 40: a network management system for identifying address information for the plurality of interconnection devices (Huff figure 4)

Claims 30, 32, 39, 41 are further embodiments of the above rejected claims and as such are rejected on the same basis.

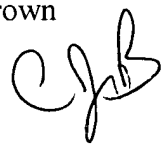
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

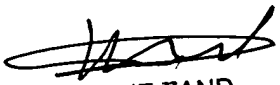
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher.J.Brown



1/5/07



KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER